The opinion in support of the decision being entered today was not written for publication in a law journal and is not binding precedent of the Board.

Paper No. 20

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte EDWARD M. SCHEIDT and C. JAY WACK

Appeal No. 2002-0121
Application No. 09/023,672

ON BRIEF

Before THOMAS, HAIRSTON and KRASS, Administrative Patent Judges.

KRASS, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the final rejection of claims 1, 2, 35, 36 and 66. Claims 3-34, 37-65 and 67-69 have been indicated by the examiner (answer-page 3) as being directed to allowable subject matter and are no longer on appeal before us.

The invention is directed to cryptographic systems. More particularly, the invention relates to formulating cryptographic

keys used to encrypt plaintext messages and decrypt ciphertext communications. A cryptographic key split combiner includes a plurality of key split generators for generating cryptographic key splits and a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key. Each of the key split generators generates key splits from the seed data.

Representative independent claim 35 is reproduced as follows:

35. A process for forming cryptographic keys, comprising:

a) generating a plurality of cryptographic key splits from seed data; and

b) randomizing the cryptographic key splits to produce a cryptographic key.

The examiner relies on the following reference:

Hirsch	5,276,738	Jan. 4, 1994

Claims 1, 2, 35, 36 and 66 stand rejected under 35 U.S.C. § 102(b) as anticipated by Hirsch.

Reference is made to the brief and answer for the respective positions of appellants and the examiner.

OPINION

Under 35 U.S.C. 102(b), a reference must disclose, explicitly or implicitly, every limitation of the claimed invention. Glaxo Inc. v. Novopharm Ltd., 52 F.3d 1043, 1047, 34 USPQ2d 1565, 1567 (Fed. Cir.), cert. denied, 516 U.S. 988 (1995).

Each of independent claims 1 and 35 requires, inter alia, the generation of a "plurality of cryptographic key splits from seed data," in one form or another. The quoted portion is from claim 35.

The examiner points to column 1, lines 57-67, of Hirsch for a teaching of this limitation. In particular, the examiner relies on Hirsch's "container multibit locations" as a teaching of the claimed plurality of key split generators. The examiner explains that the key splits in Hirsch are the individual bits of the stored input binary number rearranged as a function of random number values and that the claimed seed data from which the key splits are generated are the individual bits of the stored input binary number and the different ones of a unique sequence of

random number values (see bottom of page 8 of the answer).

We disagree. While Hirsch does generate a key value, it appears that Hirsch is describing the generation of a single modified value from a single 32-bit value by employing a scrambler which includes an array having a number of multibit container locations for storing a unique sequence of random numbers. We find absolutely nothing in Hirsch, nor has the examiner convincingly pointed to anything within Hirsch's disclosure, relating to a plurality of generators for generating cryptographic key splits from seed data, as required by the instant claims. It might be said that Hirsch generates a pseudorandom sequence from a seed, but there is nothing to indicate that Hirsch generates a plurality of cryptographic key splits from seed data.

In our view, it is unreasonable for the examiner to treat each individual bit of Hirsch's 32-bit input value as a key split, as there is no apparent reason for making such an interpretation. Even so, if we read the examiner's rationale correctly, the examiner appears to be saying that not only is each individual bit of Hirsch's 32-bit input value to be considered a claimed key split generator, but the claimed seed data from which the key splits are generated is also to be

interpreted as the individual bits of that input value. This appears to be an inconsistent and flawed rationale since, in accordance with the instant claims, the plurality of key splits must be generated from the seed data. The individual bits of the 32-bit input value of Hirsch cannot be both the key splits and the seed data from which the key splits are generated.

The examiner's decision rejecting claims 1, 2, 35, 36 and 66 under 35 U.S.C. 102(b) is reversed.

REVERSED

JAMES D. THOMAS)
Administrative Patent Judge)
)
)
)
)
KENNETH W. HAIRSTON) BOARD OF PATENT
Administrative Patent Judge) APPEALS AND
) INTERFERENCES
)
)
ERROL A. KRASS)
Administrative Patent Judge)

EK/RWK

IP STRATEGIES, PC
806 7TH STREET, NW
SUITE 301
WASHINGTON, DC 20001